IN THE CLAIMS

1. (Original) A broadcast encryption method, comprising the steps of:

allocating, to each of a plurality of subscribers, a corresponding set of subscriber keys;

broadcasting encrypted content to the plurality of subscribers using a set of broadcast keys, wherein the encrypted content is decoded by a given subscriber using the subscriber's corresponding set of subscriber keys;

modifying the set of broadcast keys, which are used for broadcasting encrypted content, by excluding compromised subscriber keys; and

updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold.

2. (Original) The method of claim 1, wherein each set of subscriber keys is encoded on a smartcard that is issued to the corresponding subscriber.

3. (Original) The method of claim 2, further comprising the steps of:

identifying a compromised smartcard; and

identifying each subscriber key contained on the compromised smartcard as a compromised key.

4. (Original) The method of claim 3, wherein a compromised smartcard comprises one of a pirate smartcard and a smartcard of an excluded subscriber.

5. (Original) The method of claim 4, wherein the step of updating comprises the steps of:

tracking a total amount of compromised cards; and

reissuing a smartcard comprising the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold.

6. (Original) The method of claim 1, wherein the first predetermined threshold is one key.

7. (Original) A broadcast encryption method, comprising the steps of:

allocating a set of subscriber keys to each of a plurality of n subscribers, wherein each set of subscriber keys is generated by randomly selecting r keys from a universal set comprising K keys;

broadcasting encrypted content to the n subscribers using a set of broadcast keys S_p selected from the universal set of keys;

identifying at least one compromised subscriber key;

adjusting S_p by excluding the at least one compromised subscriber key; and

updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold.

8. (Original) The method of claim 7, wherein the step of allocating is performed using a randomized broadcast encryption scheme wherein K is selected to ensure an (m, α) cover free family with high probability that the sets of subscriber keys corresponding to a coalition of m subscribers can not cover a fraction α of r keys comprising the set of subscriber keys of another subscriber.

9. (Original) The method of claim 8, wherein the step of broadcasting is performed using an $(\alpha r, |S_p|)$- threshold broadcast protocol.

10. (Currently amended) The method of claim 9, wherein $\alpha r=1$.

11. (Original) The method of claim 7, wherein each set of subscriber keys is encoded on a separate smartcard that is issued to the corresponding subscriber.

12. (Original) The method of claim 11, wherein the step of identifying at least one compromised subscriber key comprises the steps of:

identifying a compromised smartcard; and

identifying each subscriber key contained on the compromised card as a compromised key.

13.(Original) The method of claim 12, wherein a compromised smartcard comprises one of a pirate smartcard and a smartcard of an excluded subscriber.

14. (Original) The method of claim 12, wherein the step of updating comprises the steps of:

tracking a total amount of compromised smartcards; and

reissuing a smartcard comprising the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold ***d***.

15. (Original) The method of claim 14, wherein ***d*** is substantially equal to ***K/r***.

16. (Original) The method of claim 14, wherein the step of reissuing comprises the steps of:

generating a new key for each compromised key to update the universal set of keys; and

randomly selecting r keys from the updated universal set of keys to generate the updated set of subscriber keys.

17. (Original) The method of claim 14, wherein ***K***, ***r*** and ***d*** are selected to obtain a bound on the number of subscribers that are reissued smartcards in recarding sessions.

18. (Original) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for performing broadcast encryption, the method steps comprising:

allocating, to each of a plurality of subscribers, a corresponding set of subscriber keys;

broadcasting encrypted content to the plurality of subscribers using a set of broadcast keys, wherein the encrypted content is decoded by a given subscriber using the subscriber's corresponding set of subscriber keys;

modifying the set of broadcast keys, which are used for broadcasting encrypted content, by excluding compromised subscriber keys; and

updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold.

19. (Original) The program storage device of claim 18, further comprising instructions for performing the step of:

identifying each subscriber key contained on a compromised smartcard as a compromised key.

20. (Original) The program storage device of claim 19, wherein the instructions for performing the step of updating comprise instructions for performing the steps of:

tracking a total amount of compromised cards; and

encoding a smartcard with the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold.

21. (Original) The program storage device of claim 18, wherein the first predetermined threshold comprises one key.

22. (Original) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for broadcast encryption, the method comprising the steps of:

allocating a set of subscriber keys to each of a plurality of n subscribers, wherein each set of subscriber keys is generated by randomly selecting r keys from a universal set comprising K keys;

broadcasting encrypted content to the n subscribers using a set of broadcast keys S_p selected from the universal set of keys;

identifying at least one compromised subscriber key;

adjusting S_p by excluding the at least one compromised subscriber key; and

updating a set of subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below a first predetermined threshold.

23. (Original) The program storage device of claim 22, wherein the instructions for performing the step of allocating comprise instructions for performing a randomized broadcast encryption scheme wherein K is selected to ensure an (m, α) cover free family with high probability that the sets of subscriber keys corresponding to a coalition of m subscribers can not cover a fraction α of r keys comprising the set of subscriber keys of another subscriber.